Chapter 3
The Stored Communications Act

A. Introduction

☞ The SCA regulates how the government can obtain stored account information from network service providers such as ISPs. Whenever agents or prosecutors seek stored email, account records, or subscriber information from a network service provider, they must comply with the SCA. The SCA's classifications are summarized in the chart that appears in Section F of this chapter.

The Stored Communications Act, 18 U.S.C. §§ 2701-2712 ("SCA"), sets forth a system of statutory privacy rights for customers and subscribers of computer network service providers.[1] There are three main substantive components to this system, which serves to protect and regulate the privacy interests of network users with respect to government, network service providers, and the world at large. First, § 2703 creates a code of criminal procedure that federal and state law enforcement officers must follow to compel disclosure of stored communications from network service providers. Second, § 2702 regulates voluntary disclosure by network service providers of customer communications and records, both to government and non-government entities. Third, § 2701 prohibits unlawful access to certain stored communications; anyone who obtains, alters, or prevents authorized access to those communications is subject to criminal penalties.

The structure of the SCA reflects a series of classifications that indicate the drafters' judgments about what kinds of information implicate greater or lesser privacy interests. For example, the drafters saw greater privacy interests in the

[1] The SCA is sometimes referred to as the Electronic Communications Privacy Act. The SCA was included as Title II of the Electronic Communications Privacy Act of 1986 ("ECPA"), but ECPA itself also included amendments to the Wiretap Act and created the Pen Register and Trap and Trace Devices statute addressed in Chapter 4. *See* Pub. L. No. 99-508, 100 Stat. 1848 (1986). Although 18 U.S.C. § 2701-2712 is referred to as the "Stored Communications Act" here and elsewhere, the phrase "Stored Communications Act" appears nowhere in the language of the statute.

content of stored emails than in subscriber account information. Similarly, the drafters believed that computing services available "to the public" required more strict regulation than services not available to the public. (Perhaps this judgment reflects the view that providers available to the public are not likely to have close relationships with their customers, and therefore might have less incentive to protect their customers' privacy.) To protect the array of privacy interests identified by its drafters, the SCA offers varying degrees of legal protection depending on the perceived importance of the privacy interest involved. Some information can be obtained from providers with a subpoena; other information requires a special court order; and still other information requires a search warrant. In addition, some types of legal process require notice to the subscriber, while other types do not.

Agents and prosecutors must apply the various classifications devised by the SCA's drafters to the facts of each case to figure out the proper procedure for obtaining the information sought. First, they must classify the network service provider (*e.g.*, does the provider provide "electronic communication service," "remote computing service," or neither). Next, they must classify the information sought (*e.g.*, is the information content "in electronic storage," content held by a remote computing service, a non-content record pertaining to a subscriber, or other information enumerated by the SCA). Third, they must consider whether they are seeking to compel disclosure or seeking to accept information disclosed voluntarily by the provider. If they seek compelled disclosure, they need to determine whether they need a search warrant, a 2703(d) court order, or a subpoena to compel the disclosure. If they are seeking to accept information voluntarily disclosed, they must determine whether the statute permits the disclosure. The chart contained in Section F of this chapter provides a useful way to apply these distinctions in practice.

The organization of this chapter will follow the SCA's various classifications. Section B explains the SCA's classification structure, which distinguishes between providers of "electronic communication service" and providers of "remote computing service." Section C explains the different kinds of information that providers can divulge, such as content "in electronic storage" and "records . . . pertaining to a subscriber." Section D explains the legal process that agents and prosecutors must follow to compel a provider to disclose information. Section E looks at the flip side of this problem and explains when providers may voluntarily disclose account information. A summary chart appears in Section F. Section G discusses important issues that may arise when agents

obtain records from network providers: steps to preserve evidence, steps to prevent disclosure to subjects, Cable Act issues, and reimbursement to providers. Section H discusses the Fourth Amendment's application to stored electronic communications. Finally, Section I discusses the remedies that courts may impose following violations of the SCA.

B. Providers of Electronic Communication Service vs. Remote Computing Service

The SCA protects communications held by two defined classes of network service providers: providers of "electronic communication service," *see* 18 U.S.C. § 2510(15), and providers of "remote computing service," *see* 18 U.S.C. § 2711(2). Careful examination of the definitions of these two terms is necessary to understand how to apply the SCA.

1. Electronic Communication Service

An electronic communication service ("ECS") is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). (For a discussion of the definitions of wire and electronic communications, see Chapter 4.D.2.) For example, "telephone companies and electronic mail companies" generally act as ECS providers. *See* S. Rep. No. 99-541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3568; *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 900-03 (9th Cir. 2008) (text messaging service provider is an ECS); *In re Application of United States*, 509 F. Supp. 2d 76, 79 (D. Mass. 2007) (cell phone service provider is an ECS); *Kaufman v. Nest Seekers, LLC,* 2006 WL 2807177, at *5 (S.D.N.Y. Sept. 26, 2006) (host of electronic bulletin board is ECS); *Freedman v. America Online, Inc.*, 325 F. Supp. 2d 638, 643 n.4 (E.D. Va. 2004) (AOL is an ECS).

Any company or government entity that provides others with the means to communicate electronically can be a "provider of electronic communication service" relating to the communications it provides, regardless of the entity's primary business or function. *See Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114-15 (3d Cir. 2004) (insurance company that provided email service to employees is an ECS); *Bohach v. City of Reno*, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (city providing pager service to its police officers was a provider of ECS); *United States v. Mullins*, 992 F.2d 1472, 1478 (9th Cir. 1993) (airline that provides travel agents with computerized travel reservation system

accessed through separate computer terminals can be a provider of ECS). In *In re Application of United States,* 349 F.3d 1132, 1138-41 (9th Cir. 2003), the Ninth Circuit held that a company operating a system that enabled drivers to communicate with designated call centers over a cellular telephone network was an ECS, though it also noted that the situation would have been entirely different "if the Company merely used wire communication as an incident to providing some other service, as is the case with a street-front shop that requires potential customers to speak into an intercom device before permitting entry, or a 'drive-thru' restaurant that allows customers to place orders via a two-way intercom located beside the drive-up lane." *Id.* at 1141 n.19.

A provider cannot provide ECS with respect to a communication if the service did not provide the ability to send or receive *that* communication. *See Sega Enterprises Ltd. v. MAPHIA*, 948 F. Supp. 923, 930-31 (N.D. Cal. 1996) (video game manufacturer that accessed private email of users of another company's bulletin board service was not a provider of electronic communication service); *State Wide Photocopy, Corp. v. Tokai Fin. Servs., Inc.*, 909 F. Supp. 137, 145 (S.D.N.Y. 1995) (financing company that used fax machines and computers but did not provide the ability to send or receive communications was not provider of electronic communication service).

Significantly, a mere user of ECS provided by another is not a provider of ECS. For example, a commercial website is not a provider of ECS, even though it may send and receive electronic communications from customers. In *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1270 (N.D. Cal. 2001), the plaintiff argued that Amazon.com (to whom plaintiff sent his name, credit card number, and other identification information) was an electronic communications service provider because "without recipients such as Amazon.com, users would have no ability to send electronic information." The court rejected this argument, holding that Amazon was properly characterized as a user rather than a provider of ECS. *See id*. *See also United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003) (a home computer connected to the Internet is not an ECS); *In re Jetblue Airways Corp. Privacy Litigation*, 379 F. Supp. 2d 299, 309-10 (E.D.N.Y. 2005) (airline that operated website that enabled it to communicate with customers was not an ECS); *Dyer v. Northwest Airlines Corp.*, 334 F. Supp. 2d 1196, 1199 (D.N.D. 2004) (ECS "does not encompass businesses selling traditional products or services online"); *In re Doubleclick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 508-09 (S.D.N.Y. 2001) (distinguishing ISPs that provide ECS from websites that are users of

ECS). However, "an online business or retailer may be considered an electronic communication service provider if the business has a website that offers customers the ability to send messages or communications to third parties." *Becker v. Toca*, 2008 WL 4443050, at *4 (E.D. La. Sept. 26, 2008).

2. Remote Computing Service

The term "remote computing service" ("RCS") is defined by 18 U.S.C. § 2711(2) as "the provision to the public of computer storage or processing services by means of an electronic communications system." An "electronic communications system" is "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(14).

Roughly speaking, a remote computing service is provided by an off-site computer that stores or processes data for a customer. *See* S. Rep. No. 99-541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3564-65. For example, a service provider that allows customers to use its computing facilities in "essentially a time-sharing arrangement" provides an RCS. H.R. Rep. No. 99-647, at 23 (1986). A server that allows users to store data for future retrieval also provides an RCS. *See Steve Jackson Games, Inc. v. United States Secret Service*, 816 F. Supp. 432, 442-43 (W.D. Tex. 1993) (provider of bulletin board services was a remote computing service), *aff'd on other grounds*, 36 F.3d 457 (5th Cir. 1994). Importantly, an entity that operates a website and its associated servers is not an RCS, unless of course the entity offers a storage or processing service through the website. For example, an airline may compile and store passenger information and itineraries through its website, but these functions are incidental to providing airline reservation service, not data storage and processing service; they do not convert the airline into an RCS. *See In re Jetblue Airways Corp. Privacy Litigation*, 379 F. Supp. 2d at 310; *see also United States v. Standefer*, 2007 WL 2301760, at *5 (S.D. Cal. Aug. 8, 2007) (holding that e-gold payment website was not an RCS because e-gold customers did not use the website "to simply store electronic data" or to "outsource tasks," but instead used e-gold "to transfer gold ownership to other users").

Under the definition provided by § 2711(2), a service can only be a "remote computing service" if it is available "to the public." Services are available to the public if they are available to any member of the general population who complies with the requisite procedures and pays any requisite fees. For example,

Verizon is a provider to the public: anyone can obtain a Verizon account. (It may seem odd at first that a service can charge a fee but still be considered available "to the public," but this approach mirrors commercial relationships in the physical world. For example, movie theaters are open "to the public" because anyone can buy a ticket and see a show, even though tickets are not free.) In contrast, providers whose services are available only to those with a special relationship with the provider do not provide service to the public. For example, an employer that provides email accounts to its employees will not be an RCS with respect to those employees, because such email accounts are not available to the public. *See Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998) (interpreting the "to the public" clause in § 2702(a) to exclude an internal email system that was made available to a hired contractor but was not available to "any member of the community at large").

In *Quon v. Arch Wireless Operating Co.*, the Ninth Circuit held that a text messaging service provider was an ECS and therefore not an RCS. *See Quon*, 529 F.3d at 902-03. However, this "either/or" approach to ECS and RCS is contrary to the language of the statute and its legislative history. The definitions of ECS and RCS are independent of each other, and therefore nothing prevents a service provider from providing both forms of service to a single customer. In addition, an email service provider is certainly an ECS, but the House report on the SCA also stated that an email stored after transmission would be protected by a provision of the SCA that protects contents of communications stored by an RCS. *See* H.R. Rep. No. 99-647, at 65 (1986). One subsequent court has rejected the Ninth Circuit's analysis in *Quon* and stated that a provider "may be deemed to provide both an ECS and an RCS to the same customer." *Flagg, v. City of Detroit*, 252 F.R.D. 346, 362 (E.D. Mich. 2008). The key to determining whether the provider is an ECS or RCS is to ask what role the provider has played and is playing with respect to the communication in question.

C. Classifying Types of Information Held by Service Providers

Network service providers can store different kinds of information relating to an individual customer or subscriber. Consider the range of information that an ISP may typically store regarding one of its customers. It may have the customer's subscriber information, such as name, address, and credit card

number. It may have logs revealing when the customer logged on and off the service, the IP addresses assigned to the customer, and other more detailed logs pertaining to what the customer did while online. The ISP may also have the customer's opened, unopened, draft, and sent emails.

When agents and prosecutors wish to obtain such records, they must be able to classify these types of information using the language of the SCA. The SCA breaks the information down into three categories: (1) contents; (2) non-content records and other information pertaining to a subscriber or customer; and (3) basic subscriber and session information, which is a subset of non-content records and is specifically enumerated in 18 U.S.C. § 2703(c)(2). *See* 18 U.S.C. §§ 2510(8), 2703. In addition, as described below, the SCA creates substantially different protections for contents in "electronic storage" in an ECS and contents stored by a provider of RCS.

1. Basic Subscriber and Session Information Listed in 18 U.S.C. § 2703(c)(2)

Section 2703(c)(2) lists the categories of basic subscriber and session information:

> (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number)[.]

In general, the items in this list relate to the identity of a subscriber, his relationship with his service provider, and his basic session connection records. In the Internet context, "any temporarily assigned network address" includes the IP address used by a customer for a particular session. For example, for a webmail service, the IP address used by a customer accessing her email account constitutes a "temporarily assigned network address." This list does not include other, more extensive transaction-related records, such as logging information revealing the email addresses of persons with whom a customer corresponded.

2. Records or Other Information Pertaining to a Customer or Subscriber

Section 2703(c)(1) covers a second type of information: "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)." This is a catch-all category that includes all records that are not contents, including basic subscriber and session information described in the previous section. As one court explained, "a record means something stored or archived. The term information is synonymous with data." *In re United States*, 509 F. Supp. 2d 76, 80 (D. Mass. 2007).

Common examples of "record[s] . . . pertaining to a subscriber" include transactional records, such as account logs that record account usage; cell-site data for cellular telephone calls; and email addresses of other individuals with whom the account holder has corresponded. *See* H.R. Rep. No. 103-827, at 10, 17, 31 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3490, 3497, 3511. *See also In re Application of United States*, 509 F. Supp. 76, 80 (D. Mass. 2007) (historical cell-site information fall within scope of § 2703(c)(1)); *United States v. Allen*, 53 M.J. 402, 409 (C.A.A.F. 2000) (concluding that "a log identifying the date, time, user, and detailed internet address of sites accessed" by a user constituted "a record or other information pertaining to a subscriber or customer of such service" under the SCA); *Hill v. MCI WorldCom Commc'ns, Inc.*, 120 F. Supp. 2d 1194, 1195-96 (S.D. Iowa 2000) (concluding that the "names, addresses, and phone numbers of parties . . . called" constituted "a record or other information pertaining to a subscriber or customer of such service," not contents, for a telephone account); *Jessup-Morgan v. America Online, Inc.*, 20 F. Supp. 2d 1105, 1108 (E.D. Mich. 1998) (holding that a customer's identification information is a "record or other information pertaining to a subscriber" rather than contents). According to the legislative history of the 1994 amendments to § 2703(c), the purpose of separating the basic subscriber and session information from other non-content records was to distinguish basic subscriber and session information from more revealing transactional information that could contain a "person's entire on-line profile." H.R. Rep. No. 103-827, at 17, 31-32 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3497, 3511-12.

3. Contents and "Electronic Storage"

The contents of a network account are the actual files (including email) stored in the account. *See* 18 U.S.C. § 2510(8) ("'contents,' when used with

respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication"). For example, stored emails or voice mails are "contents," as are word processing files stored in employee network accounts. The subject lines of emails are also contents. *Cf. Brown v. Waddell*, 50 F.3d 285, 292 (4th Cir. 1995) (noting that numerical pager messages allow "an unlimited range of number-coded substantive messages" in the course of holding that the interception of pager messages requires compliance with Title III).

The SCA further divides contents into two categories: contents in "electronic storage" held by a provider of electronic communication service, and contents stored by a remote computing service. (In addition, contents that fall outside of these two categories are not protected by the SCA.) Importantly, "electronic storage" is a statutorily defined term. It does *not* simply mean storage of information by electronic means. Instead, "electronic storage" is "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17). Moreover, the definition of "electronic storage" is important because, as explained in Section D below, contents in "electronic storage" for less than 181 days can be obtained only with a warrant.

Unfortunately, as a result of the Ninth Circuit's decision in *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), there is now a split between two interpretations of "electronic storage"—a traditional narrow interpretation and an expansive interpretation supplied by the Ninth Circuit. Both interpretations are discussed below. As a practical matter, federal law enforcement within the Ninth Circuit is bound by the Ninth Circuit's decision in *Theofel*, but law enforcement elsewhere may continue to apply the traditional interpretation of "electronic storage."

As traditionally understood, "electronic storage" refers only to temporary storage made in the course of transmission by a service provider and to backups of such intermediate communications made by the service provider to ensure system integrity. It does not include post-transmission storage of communications. For example, email that has been received by a recipient's service provider but has not yet been accessed by the recipient is in "electronic storage." *See Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 461 (5th Cir. 1994). At that stage, the communication is stored as a

temporary and intermediate measure pending the recipient's retrieval of the communication from the service provider. Once the recipient retrieves the email, however, the communication reaches its final destination. If the recipient chooses to retain a copy of the accessed communication, the copy will not be in "temporary, intermediate storage" and is not stored incident to transmission. *See Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2004) (stating that email in post-transmission storage was not in "temporary, intermediate storage"). By the same reasoning, if the sender of an email maintains a copy of the sent email, the copy will not be in "electronic storage." Messages posted to an electronic "bulletin board" or similar service are also not in "electronic storage" because the website on which they are posted is the final destination for the information. *See Snow v. DirecTV, Inc.*, 2005 WL 1226158, at *3 (M.D. Fla. May 9, 2005), *adopted by* 2005 WL 1266435 (M.D. Fla. May 27, 2005), *aff'd on other grounds*, 450 F.3d 1314 (11th Cir. 2006).

Furthermore, the "backup" component of the definition of "electronic storage" refers to copies made by an ISP to ensure system integrity. As one district court explained, the backup component "protects the communication in the event the system crashes before transmission is complete. The phrase 'for purposes of backup protection of such communication' in the statutory definition makes clear that messages that are in post-transmission storage, after transmission is complete, are not covered by part (B) of the definition of 'electronic storage.'" *Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001), *aff'd in part on other grounds* 352 F.3d 107, 114 (3d Cir. 2004) (affirming the SCA portion of the district court's ruling on other grounds); *see also United States v. Weaver,* 2009 WL 2163478, at *4 (C.D. Ill. July 15, 2009) (interpreting "electronic storage" to exclude previously sent email stored by web-based email service provider); *In re Doubleclick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 511-13 (S.D.N.Y. 2001) (emphasizing that "electronic storage" should have a narrow interpretation based on statutory language and legislative intent and holding that cookies fall outside of the definition of "electronic storage" because of their "long-term residence on plaintiffs' hard drives"); H.R. Rep. No. 99-647, at 65 (1986) (noting congressional intent that opened email left on a provider's system be covered by provisions of the SCA relating to remote computing services, rather than provisions relating to communications in "electronic storage").

This narrow interpretation of "electronic storage" was rejected by the Ninth Circuit in *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), in which

the court held that email messages were in "electronic storage" regardless of whether they had been previously accessed, because it concluded that retrieved email fell within the backup portion of the definition of "electronic storage." *Id.* at 1075-77. Although the Ninth Circuit did not dispute that previously accessed email was not in temporary, intermediate storage within the meaning of § 2510(17)(A), it insisted that a previously accessed email message fell within the scope of the "backup" portion of the definition of "electronic storage," because such a message "functions as a 'backup' for the user." *Id.* at 1075. However, CCIPS has consistently argued that the Ninth Circuit's broad interpretation of the "backup" portion of the definition of "electronic storage" should be rejected. There is no way for a service provider to determine whether a previously opened email on its servers is a backup for a copy of the email stored by a user on his computer, as the service provider simply cannot know whether the underlying email remains stored on the user's computer. Essentially, the Ninth Circuit's reasoning in *Theofel* confuses "backup protection" with ordinary storage of a file.

Although prosecutors within the Ninth Circuit are bound by *Theofel*, law enforcement elsewhere may continue to apply the traditional narrow interpretation of "electronic storage," even when the data sought is within the Ninth Circuit. Recent lower court decisions addressing the scope of "electronic storage" have split between the traditional interpretation and the *Theofel* approach. *Compare United States v. Weaver,* 2009 WL 2163478, at *4 (C.D. Ill. July 15, 2009) (rejecting Theofel), *and Bansal v. Russ*, 513 F. Supp. 2d 264, 276 (E.D. Pa. 2007) (holding that access to opened email in account held by non-public service provider did not violate the SCA), *with Bailey v. Bailey*, 2008 WL 324156, at *6 (E.D. Mich. Feb. 6, 2008) (endorsing *Theofel*), *and Cardinal Health 414, Inc. v. Adams*, 482 F. Supp. 2d 967, 976 n.2 (M.D. Tenn. 2008) (same). Prosecutors confronted with *Theofel*-related issues should consult CCIPS at (202) 514-1026 for further assistance.

4. Illustration of the SCA's Classifications in the Email Context

An example illustrates how the SCA's categories work in practice outside the Ninth Circuit, where *Theofel* does not apply. Imagine that Joe sends an email from his account at work ("joe@goodcompany.com") to the personal account of his friend Jane ("jane@localisp.com"). The email will stream across the Internet until it reaches the servers of Jane's Internet service provider, here the fictional LocalISP. When the message first arrives at LocalISP, LocalISP is a provider of ECS with respect to that message. Before Jane accesses LocalISP and

retrieves the message, Joe's email is in "electronic storage." Once Jane retrieves Joe's email, she can either delete the message from LocalISP's server or else leave the message stored there. If Jane chooses to store the email with LocalISP, LocalISP is now a provider of RCS (and not ECS) with respect to the email sent by Joe. The role of LocalISP has changed from a transmitter of Joe's email to a storage facility for a file stored remotely for Jane by a provider of RCS.

Next imagine that Jane responds to Joe's email. Jane's return email to Joe will stream across the Internet to the servers of Joe's employer, Good Company. Before Joe retrieves the email from Good Company's servers, Good Company is a provider of ECS with respect to Jane's email (just like LocalISP was with respect to Joe's original email before Jane accessed it). When Joe accesses Jane's email message and the communication reaches its destination (Joe), Good Company ceases to be a provider of ECS with respect to that email (just as LocalISP ceased to be a provider of ECS with respect to Joe's original email when Jane accessed it). Unlike LocalISP, however, Good Company does not become a provider of RCS if Joe decides to store the opened email on Good Company's server. Rather, for purposes of this specific message, Good Company is a provider of neither ECS nor RCS. Good Company does not provide RCS because it does not provide services to the public. *See* 18 U.S.C. § 2711(2) ("[T]he term 'remote computing service' means the provision *to the public* of computer storage or processing services by means of an electronic communications system." (emphasis added)); *Andersen Consulting*, 991 F. Supp. at 1043. Because Good Company provides neither ECS nor RCS with respect to the opened email in Joe's account, the SCA no longer regulates access to this email, and such access is governed solely by the Fourth Amendment. Functionally speaking, the opened email in Joe's account drops out of the SCA.

Finally, consider the status of the other copies of the emails in this scenario: Jane has downloaded a copy of Joe's email from LocalISP's server to her personal computer at home, and Joe has downloaded a copy of Jane's email from Good Company's server to his office desktop computer at work. The SCA governs neither. Although these computers contain copies of emails, these copies are not stored on the server of a third-party provider of RCS or ECS, and therefore the SCA does not apply. Access to the copies of the communications stored in Jane's personal computer at home and Joe's office computer at work is governed solely by the Fourth Amendment. *See generally* Chapters 1 and 2.

As this example indicates, a single provider can simultaneously provide ECS with regard to some communications and RCS with regard to others, or ECS with regard to some communications and neither ECS nor RCS with regard to others. A chart illustrating these issues appears in Section F of this chapter. Sample language that agents may use appears in Appendices B, E, and F.

D. Compelled Disclosure Under the SCA

Section 2703 articulates the steps that the government must take to compel providers to disclose the contents of stored wire or electronic communications (including email and voice mail) and other information such as account records and basic subscriber and session information.

Section 2703 offers five mechanisms that a "government entity" can use to compel a provider to disclose certain kinds of information. The five mechanisms are as follows:

1) Subpoena;

2) Subpoena with prior notice to the subscriber or customer;

3) § 2703(d) court order;

4) § 2703(d) court order with prior notice to the subscriber or customer; and

5) Search warrant.

One feature of the compelled disclosure provisions of the SCA is that greater process generally includes access to information that cannot be obtained with lesser process. Thus, a 2703(d) court order can compel everything that a subpoena can compel (plus additional information), and a search warrant can compel the production of everything that a 2703(d) order can compel (and then some). As a result, the additional work required to satisfy a higher threshold will often be justified because it can authorize a broader disclosure. Note, however, the notice requirement must be considered separately under this analysis: a subpoena with notice to the subscriber can be used to compel information not available using a 2703(d) order without subscriber notice.

Two circumstances allow the government to compel disclosure of information under the SCA without a subpoena. First, when investigating telemarketing fraud, law enforcement may submit a written request to a service provider for

the name, address, and place of business of a subscriber or customer engaged in telemarketing. *See* 18 U.S.C. § 2703(c)(1)(D). Second, the government may compel a service provider to disclose non-content information pertaining to a customer or subscriber when the government has obtained the customer or subscriber's consent. *See* 18 U.S.C. § 2703(c)(1)(C).

1. Subpoena

The SCA permits the government to compel disclosure of the basic subscriber and session information (discussed above in Section C.1) listed in 18 U.S.C. § 2703(c)(2) using a subpoena:

> (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number)[.]

18 U.S.C. § 2703(c)(2).

Agents can also use a subpoena to obtain information that is outside the scope of the SCA. The hypothetical email exchange between Jane and Joe discussed in Section C of this chapter provides a useful example: Good Company provided neither "remote computing service" nor "electronic communication service" with respect to the opened email on Good Company's server. Accordingly, § 2703 does not impose any requirements on its disclosure, and investigators can issue a subpoena compelling Good Company to divulge the communication just as they would if the SCA did not exist. Similarly, information relating or belonging to a person who is neither a "customer" nor a "subscriber" is not protected by the SCA and may be obtained using a subpoena according to the same rationale. *Cf. Organizacion JD Ltda. v. United States Dep't of Justice*, 124 F.3d 354, 359-61 (2d Cir. 1997) (discussing the scope of the word "customer" as used in the SCA).

The legal threshold for issuing a subpoena is low. *See United States v. Morton Salt Co.*, 338 U.S. 632, 642-43 (1950). Investigators may obtain disclosure pursuant to § 2703(c)(2) using any federal or state grand jury or trial subpoena or an administrative subpoena authorized by a federal or state statute. *See* 18 U.S.C. § 2703(c)(2). For example, subpoenas authorized by the Inspector

General Act may be used. *See* 5 U.S.C. app. 3 § 6(a)(4). Of course, evidence obtained in response to a federal grand jury subpoena must be protected from disclosure pursuant to Fed. R. Crim. P. 6(e). At least one court has held that a pre-trial discovery subpoena issued in a civil case pursuant to Fed. R. Civ. P. 45 is inadequate. *See FTC v. Netscape Commc'ns Corp.*, 196 F.R.D. 559, 561 (N.D. Cal. 2000) (holding that civil discovery subpoena did not fall within the meaning of "trial subpoena"). Sample subpoena language appears in Appendix E.

2. Subpoena with Prior Notice to the Subscriber or Customer

Agents who obtain a subpoena and *either* give prior notice to the subscriber *or* comply with the delayed notice provisions of § 2705(a) may obtain:

> 1) everything that can be obtained using a subpoena without notice;
>
> 2) "the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days." 18 U.S.C. § 2703(a); and
>
> 3) "the contents of any wire or electronic communication" held by a provider of remote computing service "on behalf of . . . a subscriber or customer of such remote computing service." 18 U.S.C. § 2703(b)(1)(B)(i), § 2703(b)(2).

Outside the Ninth Circuit (which is now governed by *Theofel*), this third category will include opened and sent email. Agents outside of the Ninth Circuit can therefore obtain such email (and other stored electronic or wire communications in "electronic storage" more than 180 days) using a subpoena, provided they comply with the SCA's notice provisions. However, in light of *Theofel*, some service providers may be reluctant to produce opened or sent email less than 181 days old without a warrant. Prosecutors moving to compel compliance with a subpoena for such email should contact CCIPS at (202) 514-1026 for assistance. In the Ninth Circuit, agents can continue to subpoena communications that have been in "electronic storage" over 180 days.

The notice provisions can be satisfied by giving the customer or subscriber "prior notice" of the disclosure. *See* 18 U.S.C. § 2703(b)(1)(B). However, 18 U.S.C. § 2705(a)(1)(B) permits notice to be delayed for ninety days "upon the execution of a written certification of a supervisory official that

there is reason to believe that notification of the existence of the subpoena may have an adverse result." 18 U.S.C. § 2705(a)(1)(B). Both "supervisory official" and "adverse result" are specifically defined terms for the purpose of delaying notice. *See* 18 U.S.C. § 2705(a)(2) (defining "adverse result"); 18 U.S.C. § 2705(a)(6) (defining "supervisory official"). This provision of the SCA provides a permissible way for the government to delay notice to the customer or subscriber when notice would jeopardize a pending investigation or endanger the life or physical safety of an individual. The government may extend the delay of notice for additional 90-day periods through additional certifications that meet the "adverse result" standard of section 2705(b). *See* 18 U.S.C. § 2705(a)(4). Upon expiration of the delayed notice period, the statute requires the government to send a copy of the request or process along with a letter explaining the delayed notice to the customer or subscriber. *See* 18 U.S.C. § 2705(a)(5).

3. Section 2703(d) Order

☞ Agents need a § 2703(d) court order to obtain most account logs and most transactional records.

Agents who obtain a court order under 18 U.S.C. § 2703(d) may obtain:

> 1) anything that can be obtained using a subpoena without notice; and
>
> 2) all "record[s] or other information pertaining to a subscriber to or customer of such service (not including the contents of communications [held by providers of electronic communications service and remote computing service])." 18 U.S.C. § 2703(c)(1).

A court order authorized by 18 U.S.C. § 2703(d) may be issued by any federal magistrate, district court, or equivalent state court judge. *See* 18 U.S.C. §§ 2703(d), 2711(3). To obtain such an order,

> the governmental entity [must] offer[] specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

18 U.S.C. § 2703(d).

This standard does not permit law enforcement merely to certify that it has specific and articulable facts that would satisfy such a showing. Rather, the government must actually offer those facts to the court in the application for the order. *See United States v. Kennedy*, 81 F. Supp. 2d 1103, 1109-10 (D. Kan. 2000) (concluding that a conclusory application for a 2703(d) order "did not meet the requirements of the statute."). As the Tenth Circuit has noted, the "specific and articulable facts" standard of 2703(d) "derives from the Supreme Court's decision in [*Terry v. Ohio*, 392 U.S. 1 (1968)]." *United States v. Perrine,* 518 F.3d 1196, 1202 (10th Cir. 2008). The House Report accompanying the 1994 amendment to section 2703(d) included the following analysis:

> This section imposes an intermediate standard to protect on-line transactional records. It is a standard higher than a subpoena, but not a probable cause warrant. The intent of raising the standard for access to transactional data is to guard against "fishing expeditions" by law enforcement. Under the intermediate standard, the court must find, based on law enforcement's showing of facts, that there are specific and articulable grounds to believe that the records are relevant and material to an ongoing criminal investigation.

H.R. Rep. No. 102-827, at 31-32 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3511-12 (quoted in full in *Kennedy*, 81 F. Supp. 2d at 1109 n.8). As a practical matter, a short factual summary of the investigation and the role that the records will serve in advancing the investigation should satisfy this criterion. A more in-depth explanation may be necessary in particularly complex cases. A sample § 2703(d) application and order appears in Appendix B.

Section 2703(d) orders issued by federal courts have effect outside the district of the issuing court. The SCA permits a judge to enter 2703(d) orders compelling providers to disclose information even if the judge does not sit in the district in which the information is stored. *See* 18 U.S.C. § 2703(d) (stating that "*any court* that is a court of competent jurisdiction" may issue a 2703(d) order) (emphasis added); 18 U.S.C. § 2711(3) (stating that "'court of competent jurisdiction' has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographical limitation"); 18 U.S.C. § 3127(2) (defining "court of competent jurisdiction").

Section 2703(d) orders may also be issued by state courts. *See* 18 U.S.C. §§ 2711(3), 3127(2)(B) (defining "court of competent jurisdiction" to include

"a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device"). However, the statute provides that when a state governmental entity seeks a 2703(d) order, the order "shall not issue if prohibited by the law of such State." 18 U.S.C. § 2703(d). Moreover, although the statute explicitly allows federal courts to issue 2703(d) orders to providers outside of the court's district, it is silent on whether state courts have such authority.

4. 2703(d) Order with Prior Notice to the Subscriber or Customer

☞ Investigators can obtain everything associated with an account except for unopened email or voicemail stored with a provider for 180 days or less using a 2703(d) court order that complies with the notice provisions of § 2705.

Agents who obtain a court order under 18 U.S.C. § 2703(d), and either give prior notice to the subscriber or else comply with the delayed notice provisions of § 2705(a), may obtain:

> 1) everything that can be obtained using a § 2703(d) court order without notice;
>
> 2) "the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days," 18 U.S.C. § 2703(a); and
>
> 3) "the contents of any wire or electronic communication" held by a provider of remote computing service "on behalf of . . . a subscriber or customer of such remote computing service." 18 U.S.C. § 2703(b)(1)(B)(ii), § 2703(b)(2).

As a practical matter, except in the Ninth Circuit, this means that the government can use a 2703(d) order that complies with the prior notice provisions of § 2703(b)(1)(B) to obtain the full contents of a subscriber's account except unopened email and voicemail that have been in the account for 180 days or less. In the Ninth Circuit, which is governed by *Theofel*, agents can continue to use 2703(d) orders to obtain communications in "electronic storage" over 180 days. Following *Theofel*, some providers have resisted producing email content less than 181 days old in response to a 2703(d) order, even when the 2703(d) order is issued by a court outside the Ninth Circuit.

Prosecutors encountering this problem should contact CCIPS at (202) 514-1026 for assistance.

As an alternative to giving prior notice, law enforcement can obtain an order delaying notice for up to ninety days when notice would seriously jeopardize the investigation. *See* 18 U.S.C. § 2705(a). In such cases, prosecutors generally will obtain this order by including an appropriate request in the 2703(d) application and proposed order; sample language appears in Appendix B. Prosecutors may also apply to the court for extensions of the delay. *See* 18 U.S.C. § 2705(a)(4). The legal standards for obtaining a court order delaying notice mirror the standards for certified delayed notice by a supervisory official. *See* Section D.2., *supra*. The applicant must satisfy the court that "there is reason to believe that notification of the existence of the court order may . . . endanger[] the life or physical safety of an individual; [lead to] flight from prosecution; [lead to] destruction of or tampering with evidence; [lead to] intimidation of potential witnesses; or . . . otherwise seriously jeopardiz[e] an investigation or unduly delay[] a trial." 18 U.S.C. §§ 2705(a)(1)(A), 2705(a)(2). The applicant must satisfy this standard anew in every application for an extension of the delayed notice.

5. Search Warrant

☞ Investigators can obtain everything associated with an account with a search warrant. The SCA does not require the government to notify the customer or subscriber when it obtains information from a provider using a search warrant.

Agents who obtain a search warrant under § 2703 may obtain:

> 1) everything that can be obtained using a § 2703(d) court order with notice; and
>
> 2) "the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less." 18 U.S.C. § 2703(a).

In other words, agents can obtain any content or non-content information pertaining to an account by obtaining a search warrant "issued using the procedures described in" Fed. R. Crim. P. 41. 18 U.S.C. § 2703(a).

Search warrants issued under § 2703 have several noteworthy procedural features. First, although most search warrants obtained under Rule 41 are

limited to "a search of property . . . within the district" of the authorizing magistrate judge, search warrants under § 2703 may be issued by a federal "court with jurisdiction over the offense under investigation," even for records held in another district. *See United States v. Berkos*, 543 F.3d 392, 396-98 (7th Cir. 2008); *In re Search of Yahoo, Inc.*, 2007 WL 1539971, at *6 (D. Ariz. May 21, 2007); *In Re Search Warrant*, 2005 WL 3844032, at *5-6 (M.D. Fla. 2006) ("Congress intended 'jurisdiction' to mean something akin to territorial jurisdiction"). State courts may also issue warrants under § 2703, but the statute does not give these warrants effect outside the limits of the courts' territorial jurisdiction. Second, obtaining a search warrant obviates the need to give notice to the subscriber. *See* 18 U.S.C. § 2703(b)(1)(A); Fed. R. Crim. P. 41(f)(1)(C).

Third, investigators ordinarily do not themselves search through the provider's computers in search of the materials described in the warrant. Instead, investigators serve the warrant on the provider as they would a subpoena, and the provider produces the material specified in the warrant. *See* 18 U.S.C. § 2703(g) (stating that the presence of an officer is not required for service or execution of a § 2703 warrant); *United States v. Bach*, 310 F.3d 1063, 1068 (8th Cir. 2002) (finding search of email by ISP without presence of law enforcement did not violate Fourth Amendment).

Fourth, a two-step process is often used to obtain the content of communications under a § 2703 warrant. First, the warrant directs the service provider to produce all email from within the specified account or accounts. Second, the warrant authorizes law enforcement to review the information produced to identify and copy information that falls within the scope of the particularized "items to be seized" under the warrant.

Otherwise, as a practical matter, § 2703 search warrants are obtained much like Rule 41 search warrants. As with a typical Rule 41 warrant, investigators must draft an affidavit and a proposed warrant that complies with Rule 41.

E. Voluntary Disclosure

☞ Providers of services not available "to the public" may freely disclose both contents and other records relating to stored communications. The SCA imposes restrictions on voluntary disclosures by providers of services to the public, but it also includes exceptions to those restrictions.

The voluntary disclosure provisions of the SCA appear in 18 U.S.C. § 2702. These provisions govern when a provider of RCS or ECS can disclose contents and other information voluntarily, both to the government and non-government entities. If the provider may disclose the information to the government and is willing to do so voluntarily, law enforcement does not need to obtain a legal order to compel the disclosure. If the provider either may not or will not disclose the information, agents must rely on compelled disclosure provisions and obtain the appropriate legal orders.

When considering whether a provider of RCS or ECS can disclose contents or records, the first question is whether the relevant service offered by the provider is available "to the public." *See* Section B, above. If the provider does not provide the applicable service "to the public," then the SCA does not place any restrictions on disclosure. *See* 18 U.S.C. § 2702(a). For example, in *Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041 (N.D. Ill. 1998), the petroleum company UOP hired the consulting firm Andersen Consulting and gave Andersen employees accounts on UOP's computer network. After the relationship between UOP and Andersen soured, UOP disclosed to the *Wall Street Journal* emails that Andersen employees had left on the UOP network. Andersen sued, claiming that the disclosure of its contents by the provider UOP had violated the SCA. The district court rejected the suit on the ground that UOP did not provide an electronic communication service to the public:

> [G]iving Andersen access to [UOP's] e-mail system is not equivalent to providing e-mail to the public. Andersen was hired by UOP to do a project and as such, was given access to UOP's e-mail system similar to UOP employees. Andersen was not any member of the community at large, but a hired contractor.

Id. at 1043. Because UOP did not provide services to the public, the SCA did not prohibit disclosure of contents belonging to UOP's "subscribers." *See id.*

If the services offered by the provider *are* available to the public, then the SCA forbids both the disclosure of contents to any third party and the disclosure of other records *to any governmental entity* unless a statutory exception applies. Even a public provider may disclose customers' *non-content* records freely to any person other than a government entity. *See* 18 U.S.C. §§ 2702(a)(3), (c)(6). Section 2702(b) contains exceptions for disclosure of contents, and § 2702(c) contains exceptions for disclosure of other customer records.

The SCA allows the voluntary disclosure of contents when:

> 1) the disclosure is made to the intended recipient of the communication, with the consent of the sender or intended recipient, to a forwarding address, or pursuant to specified legal process, § 2702(b)(1)-(4);
>
> 2) in the case of a remote computing service, the disclosure is made with the consent of a subscriber, § 2702(b)(3);[2]
>
> 3) the disclosure "may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service," § 2702(b)(5);
>
> 4) the disclosure is submitted "to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A," § 2702(b)(6);
>
> 5) the disclosure is made to a law enforcement agency "if the contents . . . were inadvertently obtained by the service provider . . . [and] appear to pertain to the commission of a crime," § 2702(b)(7); or
>
> 6) the disclosure is made to a governmental entity, "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency." § 2702(b)(8).

The SCA provides for the voluntary disclosure of non-content customer records by a provider to a governmental entity when:

[2] *See also Quon*, 529 F.3d at 900-03 (holding that text messaging service provider did not provide remote computing service and thus could not disclose users' communications to the city that subscribed to its service).

1) the disclosure is made "with the lawful consent of the customer or subscriber," or "as otherwise authorized in section 2703," § 2702(c)(1)-(2);

2) the disclosure "may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service," § 2702(c)(3);

3) the disclosure is made to a governmental entity, "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency," § 2702(c)(4); or

4) the disclosure is made "to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A." § 2702(c)(5).

In general, these exceptions permit disclosure by a provider to the public when the needs of public safety and of service providers themselves outweigh privacy concerns of customers, or else when disclosure is unlikely to pose a serious threat to privacy interests.

F. Quick Reference Guide

	Voluntary Disclosure Allowed?		How to Compel Disclosure	
	Public Provider	**Non-Public**	**Public Provider**	**Non-Public**
Basic subscriber, session, and billing information•	No, unless §2702(c) exception applies *§ 2702(a)(3)*	Yes *§ 2702(a)(3)*	Subpoena; 2703(d) order; or search warrant *§ 2703(c)(2)*	Subpoena; 2703(d) order; or search warrant *§ 2703(c)(2)*
Other transactional and account records	No, unless §2702(c) exception applies *§ 2702(a)(3)*	Yes *§ 2702(a)(3)*	2703(d) order or search warrant *§ 2703(c)(1)*	2703(d) order or search warrant *§ 2703(c)(1)*
Retrieved communications and the content of other stored files#	No, unless § 2702(b) exception applies *§ 2702(a)(2)*	Yes *§ 2702(a)(2)*	Subpoena with notice; 2703(d) order with notice; or search warrant* *§ 2703(b)*	Subpoena; SCA does not apply* *§ 2711(2)*
Unretrieved communications, including email and voice mail (in electronic storage more than 180 days)†	No, unless § 2702(b) exception applies *§ 2702(a)(1)*	Yes *§ 2702(a)(1)*	Subpoena with notice; 2703(d) order with notice; or search warrant *§ 2703(a), (b)*	Subpoena with notice; 2703(d) order with notice; or search warrant *§ 2703(a), (b)*
Unretrieved communications, including email and voice mail (in electronic storage 180 days or less)†	No, unless § 2702(b) exception applies *§ 2702(a)(1)*	Yes *§ 2702(a)(1)*	Search warrant *§ 2703(a)*	Search warrant *§ 2703(a)*

- • *See* 18 U.S.C. § 2703(c)(2) for listing of information covered. This information includes local and long distance telephone connection records and records of session times and durations as well as IP addresses assigned to the user during the Internet connections.
- † Includes the content of voice communications.
- * For investigations occurring in the Ninth Circuit, *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), requires use of a search warrant unless the communications have been in storage for more than 180 days. Some providers follow *Theofel* even outside the Ninth Circuit; contact CCIPS at (202) 514-1026 if you have an appropriate case to litigate this issue.

G. Working with Network Providers: Preservation of Evidence, Preventing Disclosure to Subjects, Cable Act Issues, and Reimbursement

Law enforcement officials who procure records under the SCA quickly learn the importance of communicating with network service providers. Communication is necessary because every network provider works differently. Some providers retain very complete records for a long period of time; others retain few records, or even none. Some providers can comply easily with law enforcement requests for information; others struggle to comply with even simple requests. These differences result from varied philosophies, resources, hardware, and software among network service providers. Because of these differences, it is often advisable for agents to communicate with a network service provider (or review the provider's law enforcement compliance guide) to learn how the provider operates *before* obtaining a legal order that compels the provider to act.

The SCA contains two provisions designed to aid law enforcement officials working with network service providers. When used properly, these provisions help ensure that providers will not delete needed records or notify others about the investigation.

1. Preservation of Evidence under 18 U.S.C. § 2703(f)

☞ Agents may direct providers to preserve existing records pending the issuance of compulsory legal process. Such requests have no prospective effect, however.

In general, no law regulates how long network service providers must retain account records in the United States. Some providers retain records for months, others for hours, and others not at all. As a result, some evidence may be destroyed or lost before law enforcement can obtain the appropriate legal order compelling disclosure. For example, suppose that a crime occurs on Day 1, agents learn of the crime on Day 28, begin work on a search warrant on Day 29, and obtain the warrant on Day 32, only to learn that the network service provider deleted the records in the ordinary course of business on Day 30. To minimize the risk that evidence will be lost, the SCA permits the government to direct providers to "freeze" stored records and communications pursuant to 18 U.S.C. § 2703(f). Specifically, § 2703(f)(1) states:

> A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

There is no legally prescribed format for § 2703(f) requests. While a simple phone call should be adequate, a fax or an email is safer practice because it both provides a paper record and guards against misunderstanding. Upon receipt of the government's request, the provider must retain the records for 90 days, renewable for another 90-day period upon a government request. *See* 18 U.S.C. § 2703(f)(2). A sample § 2703(f) letter appears in Appendix C.

Agents who send § 2703(f) letters to network service providers should be aware of two limitations. First, § 2703(f) letters should not be used prospectively to order providers to preserve records not yet created. If agents want providers to record information about future electronic communications, they should comply with the electronic surveillance statutes discussed in Chapter 4.

A second limitation of § 2703(f) is that some providers may be unable to comply effectively with § 2703(f) requests, or they may be unable to comply without taking actions that potentially could alert a suspect. In such a situation, the agent must weigh the benefit of preservation against the risk of alerting the subscriber. The key here is effective communication: agents should communicate with the network service provider before ordering the provider to take steps that may have unintended adverse effects. Investigators with questions about a provider's practices may also contact CCIPS at (202) 514-1026 for further assistance.

2. Orders Not to Disclose the Existence of a Warrant, Subpoena, or Court Order

Section § 2705(b) states:

> A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period

> as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—
>
> (1) endangering the life or physical safety of an individual;
>
> (2) flight from prosecution;
>
> (3) destruction of or tampering with evidence;
>
> (4) intimidation of potential witnesses; or
>
> (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

18 U.S.C. § 2705(b).

This language permits agents to apply for a court order directing network service providers not to disclose the existence of legal process whenever the government itself has no legal duty to notify the customer or subscriber of the process. If the relevant process is a 2703(d) order or 2703 warrant, agents can simply include appropriate language in the application and proposed order or warrant. If agents instead seek to compel the disclosure of information using a subpoena, they must apply separately for this order.

3. The Cable Act, 47 U.S.C. § 551

☞ The Cable Act restricts government access to cable operator records only when the records relate to ordinary cable services. It does not restrict government access to records relating to Internet access or telephone service provided by a cable operator.

In 1984, Congress passed the Cable Communications Policy Act ("the Cable Act"), 47 U.S.C. § 521 *et seq.* Originally, 47 U.S.C. § 551 set forth a restrictive system of rules governing law enforcement access to records possessed by a cable company. Under these rules, even a search warrant was insufficient to gain access to cable company records. The government could obtain "personally identifiable information concerning a cable subscriber" only by overcoming a heavy burden of proof at an in-court adversary proceeding, as specified in 47 U.S.C. § 551(h).

After the 1984 passage of the Cable Act, cable companies began to provide Internet access and telephone service. Some cable companies asserted that the stringent disclosure restrictions of the Cable Act governed not only their provision of traditional cable programming services, but also their provision of Internet and telephone services. Congress responded by amending the Cable Act to specify that its disclosure restrictions apply only to records revealing what ordinary cable television programming a customer purchases, such as particular premium channels or "pay per view" shows. *See* USA-PATRIOT Act § 211, 115 Stat. 272, 283-84 (2001). In particular, cable operators may disclose subscriber information to the government pursuant to the SCA, Title III, and the Pen/Trap statute, except for "records revealing cable subscriber selection of video programming." 47 U.S.C. § 551(c)(2)(D). Records revealing subscriber selection of video programming remain subject to the restrictions of 47 U.S.C. § 551(h).[3]

4. Reimbursement

☞ When a government entity obtains information pursuant to the SCA, the network provider may be entitled to reimbursement for its reasonable costs incurred in supplying the information.

In general, persons and entities are not entitled to reimbursement for complying with federal legal process unless there is specific federal statutory authorization. *See Blair v. United States,* 250 U.S. 273, 281 (1919) (discussing possibility of reimbursement for grand jury testimony). "It is beyond dispute that there is in fact a public obligation to provide evidence . . . and that this obligation persists no matter how financially burdensome it may be." *Hurtado v. United States*, 410 U.S. 578, 589 (1973) (stating that the Fifth Amendment does not require compensation for the performance of a public duty). However, in many (but not all) circumstances, the SCA requires government entities obtaining the contents of communications, records, or other information pursuant to the SCA to reimburse the disclosing person or entity. *See* 18 U.S.C. § 2706.

Section 2706 generally obligates government entities "obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704" to pay the service provider "a fee for reimbursement for such costs

[3] The Satellite Home Viewer Extension and Reauthorization Act of 2004 (SHVERA) was based on the original Cable Act and contains nearly identical provisions governing disclosure of customer records by satellite television providers. *See* 47 U.S.C. § 338(i).

as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information." 18 U.S.C. § 2706(a). Significantly, this section only requires reimbursement when the government actually obtains communication content, records, or other information. Thus, the government is not required to pay for costs incurred by a provider in responding to a 2703(f) preservation letter unless the government later obtains the preserved records.

The amount of the fee required under § 2706(a) "shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court." 18 U.S.C. § 2706(b). In practice, if the service provider seeks what appears to be unreasonably high reimbursement costs, the government should demand a detailed accounting of costs incurred by activity. A cost accounting will help ensure that the provider is not seeking reimbursement for indirect costs or activities that were not reasonably necessary to the production.

In addition, the SCA contains a reimbursement exception that precludes reimbursement in specific circumstances. The reimbursement requirement "does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703," unless a court determines that the information sought by the government is "unusually voluminous" or "caused an undue burden on the provider." 18 U.S.C. § 2706(c).

The reimbursement exception of § 2706(c) applies only to records and other information "maintained by" a communications common carrier. In *Ameritech Corp. v. McCann*, 403 F.3d 908, 912 (7th Cir. 2005), the Seventh Circuit held that reports of who placed calls to a specified customer were not "maintained by" Ameritech. Ameritech's computer system recorded calls made by a customer, but it did not automatically keep or generate a list of the calls made to a customer. Compiling such a list required substantial computation time. According to the court, Ameritech "maintains" bills and equivalent statements, and the government can therefore get such "raw information" for free. However, when the government requires Ameritech to create a report, the government must provide compensation. Prosecutors outside the Seventh Circuit are not bound by *Ameritech*, and there is a reasonably strong argument that its interpretation of § 2706(c) is flawed. Under this alternative interpretation, any information stored by a carrier is "maintained by" the

carrier, and questions regarding the difficulty of producing information can be evaluated under the "undue burden" standard of § 2706(c).

H. Constitutional Considerations

Defendants sometimes raise constitutional challenges to compelled disclosure of information from communication service providers. They typically argue that use of a 2703(d) order or a subpoena (rather than a warrant) to compel disclosure of information violated the Fourth Amendment. These claims fail for two reasons. First, the defendant may have no reasonable expectation of privacy in the information obtained from the service provider. Second, the Fourth Amendment generally permits the government to compel a provider to disclose information in an account when the provider has access to and control over the targeted information, regardless of whether the account user has a reasonable expectation of privacy in the targeted information.

It is now well established that a customer or subscriber has no reasonable expectation of privacy in her subscriber information or transactional records. In *United States v. Miller*, 425 U.S. 435 (1976), the Supreme Court held that a defendant had no reasonable expectation of privacy in his bank records because the records were not his "private papers" but were "the business records of the banks" in which the defendant could "assert neither ownership nor possession." *Id*. at 440. The Court explained that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *Id.* at 443 (citing *Hoffa v. United States*, 385 U.S. 293, 302 (1966)). The Court relied upon the principles of *Miller* in *Smith v. Maryland*, 442 U.S. 735 (1979), in which it held that a defendant had no reasonable expectation of privacy in dialed telephone numbers obtained from the phone company. *Id.* at 745-46.

Courts have now extended this *Miller/Smith* analysis to network accounts, holding that individuals retain no Fourth Amendment privacy interest in subscriber information and transactional records. *See United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) ("Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation."); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (email and Internet users have no reasonable expectation of privacy in source or destination addresses of email or the IP addresses of websites visited); *Guest v. Leis*, 255 F.3d 325,

336 (6th Cir. 2001) (finding no Fourth Amendment protection for network account holders' subscriber information obtained from communication service provider).

In contrast, whether a user has a reasonable expectation of privacy in the contents of communications stored in her account will depend on the facts and circumstances associated with the account. In *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 906 (9th Cir. 2008), the Ninth Circuit rejected "a monolithic view of text message users' reasonable expectation of privacy," explaining that "this is necessarily a context-sensitive inquiry." *Compare Quon*, 529 F.3d at 906-08 (finding reasonable expectation of privacy in pager messages based on an "informal policy that the text messages would not be audited"), *and Wilson v. Moreau*, 440 F. Supp. 2d 81, 108 (D.R.I. 2006) (finding reasonable expectation of privacy in content of Yahoo! email account), aff'd, 492 F.3d 50 (1st Cir. 2007), *with Biby v. Board of Regents*, 419 F.3d 845, 850-51 (8th Cir. 2005) (university policy stating that computer files and emails may be searched in response to litigation discovery requests eliminated computer user's reasonable expectation of privacy) *and Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001) (finding that disclaimer on private bulletin board service defeated expectation of privacy in postings). *See also United States v. Young*, 350 F.3d 1302, 1307-08 (11th Cir. 2003) (Federal Express customer had no reasonable expectation of privacy in the contents of a package based on terms of service authorizing Federal Express to inspect packages).

Critically, however, even if a user has a reasonable expectation of privacy in an item, a subpoena may be used to compel the production of the item, provided the subpoena is reasonable. *See United States v. Palmer*, 536 F.2d 1278, 1281-82 (9th Cir. 1976). The Fourth Amendment imposes a probable cause requirement *only* on the issuance of warrants. *See* U.S. Const. amend.-IV ("and no Warrants shall issue, but upon probable cause"). A century of Supreme Court case law demonstrates that reasonable subpoenas comply with the Fourth Amendment. *See Wilson v. United States*, 221 U.S. 361, 376 (1911) ("there is no unreasonable search and seizure when a [subpoena], suitably specific and properly limited in its scope, calls for the production of documents which, as against their lawful owner to whom the writ is directed, the party procuring its issuance is entitled to have produced"); *Oklahoma Press Publ'g Co. v. Walling*, 327 U.S. 186, 208 (1946); *United States v. Dionisio*, 410 U.S. 1, 9-12 (1973); *Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 414-15 (1984). The rule for when a subpoena is reasonable and thus complies with the Fourth

Amendment is also well-established: "the Fourth Amendment requires that the subpoena be sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome." *Donovan*, 464 U.S. at 415 (quoting *See v. City of Seattle*, 387 U.S. 541, 549 (1967)). Finally, the Fourth Amendment does not require that notice be given to the target of an investigation in third-party subpoena cases. *See SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743, 749-51 (1984).

In general, the cases indicate that the government may compel an entity to disclose any item that is within its control and that it may access. *See United States v. Barr*, 605 F. Supp. 114, 119 (S.D.N.Y. 1985) (subpoena served on private third-party mail service for the defendant's mail in the third party's possession); *Schwimmer v. United States*, 232 F.2d 855, 861-63 (8th Cir. 1956) (subpoena served on third-party storage facility for the defendant's private papers in the third party's possession); *Newfield v. Ryan*, 91 F.2d 700, 702-05 (5th Cir. 1937) (subpoena served on telegraph company for copies of defendants' telegrams in the telegraph company's possession). This rule is supported both by the rule that a party with "joint access or control for most purposes" may consent to a search, *see United States v. Matlock*, 415 U.S. 164, 171 n.7 (1974), and also by the rule that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *Miller*, 425 U.S. at 443.

As a practical matter, there is good reason to believe that network service providers will typically have sufficient access to and control over stored communications on their networks to produce the communications in response to compulsory process. Terms of service used by network service providers often establish that the provider has authority to access and disclose subscriber email. For example, at the time of this writing, Yahoo!'s terms of service confirm its right in its "sole discretion to pre-screen, refuse, or remove any Content that is available via the Yahoo! Services," as well as to access and disclose email to comply with legal process. Terms of service similar to Yahoo!'s were sufficient to establish Federal Express's common authority over the contents of a package in *Young*: the Eleventh Circuit concluded that because Federal Express retained the right to inspect packages, it had authority to consent to a government request to search the package without a warrant. *Young*, 350 F.3d at 1309. *See generally Warshak v. United States*, 532 F.3d 521, 527 (6th Cir. 2008) (en banc) (noting the range of terms of service used by different providers). In addition, service providers typically exercise actual authority to access the content of

communications stored on their networks. Major providers regularly screen for spam, malicious code, and child pornography. Some, such as Gmail, screen the content of email in order to target advertising at the account holder.

CCIPS has assisted many prosecutors facing constitutional challenges to the SCA, and prosecutors confronted with such challenges are encouraged to consult with CCIPS at (202) 514-1026 for further assistance.

I. Remedies

Suppression is not a remedy for nonconstitutional SCA violations. However, the SCA does create a cause of action for civil damages.

1. Suppression

The SCA does not provide a suppression remedy. *See* 18 U.S.C. § 2708 ("The [damages] remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter."). Accordingly, nonconstitutional violations of the SCA do not result in suppression of the evidence. *See United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008) ("[V]iolations of the ECPA do not warrant exclusion of evidence."); *United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003); *United States v. Smith*, 155 F.3d 1051, 1056 (9th Cir. 1998) ("[T]he Stored Communications Act expressly rules out exclusion as a remedy"); *United States v. Ferguson*, 508 F. Supp. 2d 7, 10 (D.D.C. 2007); *United States v. Sherr*, 400 F. Supp. 2d 843, 848 (D. Md. 2005); *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) ("[S]uppression is not a remedy contemplated under the ECPA."); *United States v. Hambrick*, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999) ("Congress did not provide for suppression where a party obtains stored data or transactional records in violation of the Act."), *aff'd*, 225 F.3d 656, 2000 WL 1062039 (4th Cir. 2000) (unpublished); *United States v. Reyes*, 922 F. Supp. 818, 837-38 (S.D.N.Y. 1996) ("Exclusion of the evidence is not an available remedy for this violation of the ECPA. . . . The remedy for violation of [18 U.S.C. § 2701-11] lies in a civil action.").

As discussed previously in Section H, defendants occasionally have claimed that section 2703's procedures for compelled disclosure violate the Fourth Amendment. However, even if a court were to hold section 2703 unconstitutional in some circumstances, suppression would likely not be a proper remedy. In *Illinois v. Krull*, 480 U.S. 340, 349 (1987), the Supreme

Court held that the exclusionary rule did not apply to evidence obtained in "objectively reasonable reliance on a statute." Reliance on section 2703 likely satisfies this standard, as the only decision thus far to have held section 2703 unconstitutional was reversed on appeal. *See Warshak v. United States*, 532 F.3d 521 (6th Cir. 2008) (en banc). In addition, when a defendant moves to suppress based on a claim that the SCA's procedures are unconstitutional, the court may conclude that the government's reliance on the SCA was objectively reasonable and deny the suppression motion without ruling on the constitutionality of the SCA. *See Krull*, 480 U.S. at 357 n.13; *United States v. Vanness*, 342 F.3d 1093, 1098 (10th Cir. 2003). Courts have adopted this approach in two cases in which the defendants argued that the SCA was unconstitutional. *See United States v. Warshak*, 2007 WL 4410237, at *5 (S.D. Ohio Dec. 13, 2007); *United States v. Ferguson,* 508 F. Supp. 2d 7, 9-10 (D.D.C. 2007).

2. Civil Actions and Disclosures

Although the SCA does not provide a suppression remedy for statutory violations, it does provide for civil damages (including, in some cases, punitive damages), as well as the prospect of disciplinary actions against officers and employees of the United States who have engaged in willful violations of the statute. *See, e.g.*, *Freedman v. American Online, Inc.*, 303 F. Supp. 2d 121 (D. Conn. 2004) (granting summary judgment on liability under the SCA against police officers who served on AOL a purported search warrant that had not been signed by a judge). The Ninth Circuit has held that the SCA does not impose secondary liability for aiding and abetting an SCA violation or conspiring to violate the SCA. *See Freeman v. DirecTV, Inc.*, 457 F.3d 1001, 1006 (9th Cir. 2006). Thus, liability under the SCA for a violation of the voluntary disclosure provisions of section 2702 is limited to service providers. *See id.* at 1006.

Liability and discipline can result not only from violations of the rules already described in this chapter, but also from the improper disclosure of some kinds of SCA-related information. Information that is obtained pursuant to § 2703 and that qualifies as a "record" under 5 U.S.C. § 552a(a) can be disclosed by an officer or governmental entity only "in the proper performance of the official functions of the officer or governmental entity making the disclosure." 18 U.S.C. § 2707(g). Other disclosures of such information by an officer or governmental entity are unlawful unless the information has been previously and lawfully disclosed to the public. *See id.*

The SCA includes separate provisions for suits against the United States and suits against any other person or entity. Section 2707 permits a "person aggrieved" by SCA violations that result from knowing or intentional conduct to bring a civil action against the "person or entity, other than the United States, which engaged in that violation." 18 U.S.C. § 2707(a). Relief can include money damages no less than $1,000 per person, equitable or declaratory relief, and a reasonable attorney's fee plus other reasonable litigation costs. 18 U.S.C. § 2707(b), (c). Willful or intentional violations can also result in punitive damages, *see* § 2707(c), and employees of the United States may be subject to disciplinary action for willful or intentional violations. *See* § 2707(d). A good faith reliance on a court order or warrant, grand jury subpoena, legislative authorization, or statutory authorization provides a complete defense to any civil or criminal action brought under the SCA. *See* § 2707(e). Qualified immunity may also be available. *See* Chapter 4.E.2.

Suits against the United States may be brought under 18 U.S.C. § 2712 for willful violations of the SCA, Title III, or specified sections of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 *et seq.* This section authorizes courts to award actual damages or $10,000, whichever is greater, and reasonable litigation costs. Section 2712 also defines procedures for suits against the United States and a process for staying proceedings when civil litigation would adversely affect a related investigation or criminal prosecution. *See* 18 U.S.C. § 2712 (b), (e).